

## DESCRIPTION

## Content playback device

## 5 TECHNICAL FIELD

The present invention relates to content playback techniques capable of protecting copyrighted works.

## BACKGROUND ART

10 Recording media, e.g. DVDs, on which copyrighted works such as movies and music are recorded in digital form, are widely used in recent years.

DVDs employ a system called CSS (Content Scrambling System) for protecting content from unauthorized copying. According to CSS, information unique to a DVD is stored on the DVD, and a title key is created from this information and information held in a player. Encrypted content recorded on the DVD is decrypted using this title key, and the decrypted content is played back (see Japanese Patent Application Publication H05-257816 as one example).

20 Meanwhile, a content delivery system that uses DRM (Digital Rights Management) is becoming common in recent years. According to DRM, a license is provided separately from encrypted content. The license contains a license key and a use condition. The encrypted content is decrypted

25

using the license key and the decrypted content is played back, based on the use condition.

In DRM, content and a license are distributed via a network. Further, attempts are recently being made to  
5 distribute content using a storage-type broadcast system called server broadcasting.

In view of this, there is a growing need to suitably apply DRM to content distribution that utilizes recording media such as the above.

10

#### DISCLOSURE OF THE INVENTION

To meet the above need, the present invention aims to provide a content playback device, a content playback method, and a computer program which can, when decrypting  
15 encrypted content recorded on a recording medium and playing the decrypted content, protect the content according to DRM.

The above aim can be achieved by a content playback device for decrypting encrypted content recorded on a  
20 recording medium and playing back the decrypted content, including: a read unit operable to read media information unique to the recording medium, from the recording medium; a judgment unit operable to acquire contract information relating to a contract for use of the encrypted content,  
25 and judge, based on the acquired contract information,

whether the encrypted content is permitted to be used;  
a generation unit operable to generate a content key based  
on the read media information and the acquired contract  
information, if the encrypted content is judged as being  
5 permitted to be used; a decryption unit operable to read  
the encrypted content from the recording medium, and  
decrypt the encrypted content using the generated content  
key; and a playback unit operable to play back the decrypted  
content.

10       According to this construction, the content key is  
generated based on the media information read from the  
recording medium and the separately acquired contract  
information, and the encrypted content recorded on the  
recording medium is decrypted using the generated content  
15 key. This enables a copyright on content which is  
distributed via recording media, to be secured by applying  
DRM.

Here, the media information may show a media key which  
is assigned to the recording medium, wherein the contract  
20 information shows a license key which is assigned to the  
contract, and the generation unit generates the content  
key based on the media key shown by the media information  
and the license key shown by the contract information.

According to this construction, the content key can  
25 be generated reliably based on the media key and the license

key.

Here, the contract information may include a use condition of the encrypted content, wherein the judgment unit judges whether the encrypted content is permitted  
5 to be used, based on the use condition included in the contract information.

According to this construction, the usability of the encrypted content is judged according to the use condition included in the contract information. As a result, the  
10 content can be protected from use that does not conform to the use condition.

Here, the recording medium may store generation method information in correspondence with the encrypted content, the generation method information showing whether  
15 the content key is to be generated using the license key, using the media key, or using both the license key and the media key, wherein the generation unit reads the generation method information from the recording medium, and generates the content key according to the read  
20 generation method information.

According to this construction, the content key can be generated using the appropriate generation method according to the generation method information stored on the recording medium.

25 Here, if the generation method information shows that



the content key is to be generated using both the license key and the media key, the generation unit may apply a one-way function to the license key and the media key to generate the content key.

5           According to this construction, the one-way function is applied to the license key and the media key, with it being possible to obtain a unique content key.

          Here, the contract information may include the license key, as the content key, which has been encrypted  
10   using the media key, wherein if the generation method information shows that the content key is to be generated using both the license key and the media key, the generation unit decrypts the encrypted license key using the media key to generate the content key.

15           According to this construction, the encrypted license key is decrypted using the media key, as a result of which a unique content key can be obtained.

          Here, the media information may include the media key which has been encrypted, wherein the generation unit  
20   decrypts the encrypted media key to obtain the media key.

          According to this construction, the encrypted media key is decrypted to obtain the media key. This ensures the confidentiality of the media key.

          Here, the media key may have been encrypted using  
25   device information unique to the content playback device,

wherein the generation unit reads the device information held in the content playback device, and decrypts the encrypted media key using the read device information.

According to this construction, the encrypted media  
5 key is decrypted using the device information held in the content playback device. Which is to say, only the content playback device is allowed to decrypt the encrypted media key, with it being possible to ensure the confidentiality of the media key.

10 Here, the recording medium may store a contract identifier for identifying the contract information, in correspondence with the encrypted content, wherein the judgment unit reads the contract identifier from the recording medium, and acquires the contract information  
15 identified by the read contract identifier.

According to this construction, the contract information corresponding to the encrypted content can be reliably acquired using the contract identifier stored on the recording medium.

20 Here, the recording medium may store a content identifier for identifying the encrypted content, wherein the judgment unit reads the content identifier from the recording medium, and acquires the contract information corresponding to the read content identifier.

25 According to this construction, the contract

information corresponding to the encrypted content can be reliably acquired using the content identifier stored on the recording medium.

Here, the judgment unit may include: a storage unit  
5 operable to store the contract information beforehand;  
and a judging unit operable to read the contract information from the storage unit, and judge, based on the read contract information, whether the encrypted content is permitted to be used.

10 According to this construction, the content playback device stores the contract information beforehand, which eases the acquisition of the contract information.

Here, the contract information may be stored on another recording medium, in correspondence with the  
15 encrypted content, wherein the judgment unit acquires the contract information by reading the contract information from the other recording medium.

According to this construction, the contract information is acquired from the other recording medium.  
20 Accordingly, only a user who has the other recording medium and is capable of connecting the other recording medium to the content playback device is allowed to use the contract information. In this way, the use of the contract information can be restricted to thereby prohibit  
25 unauthorized use.

Here, the content playback device may be connected, via a network, to a server device for delivering the contract information, wherein the judgment unit acquires the contract information by receiving the contract information from the server device.

According to this construction, the contract information is acquired from the server device via the network. In this way, the acquisition of the contract information can be performed easily.

Here, the generation unit may be constituted by a removable module.

According to this construction, only a user who has the module and is capable of connecting the module to the content playback device is allowed to generate the content key. By such restricting the generation of the content key, unauthorized use can be prevented.

Here, the generation unit and the judgment unit may perform mutual authentication, wherein the judgment unit outputs the contract information to the generation unit, if the judgment unit has succeeded in authenticating the generation unit, and the generation unit receives the contract information from the judgment unit and generates the content key, if the generation unit has succeeded in authenticating the judgment unit.

According to this construction, the generation unit

and the judgment unit mutually authenticate each other, to thereby eliminate any invalid generation or judgment unit.

Here, the generation unit may store a first module identifier for identifying an invalid module, acquire an  
5 identifier for identifying the judgment unit, compare the acquired identifier with the first module identifier, and refuse to receive the contract information from the judgment unit if the acquired identifier matches the first  
10 module identifier.

According to this construction, any invalid judgment unit can be eliminated.

Here, the recording medium may store a second module identifier for identifying an invalid module, wherein the  
15 judgment unit reads the second module identifier from the recording medium, acquires an identifier for identifying the generation unit, compares the acquired identifier with the second module identifier, and refuses to output the contract information to the generation unit if the acquired  
20 identifier matches the second module identifier.

According to this construction, any invalid generation unit can be eliminated.

In recent years, BDs are proposed as media that can replace conventional DVDs. BDs have a capacity of about  
25 five times that of DVDs, and can store not only conventional

SD video but also HD video.

Like CSS used by conventional DVDs, BDs employ a mechanism whereby a media key is generated from information which is held by a player and information which is unique to a medium and is stored on the medium. Content is encrypted using such a media key, and the encrypted content is recorded on the medium. In this way, the content is protected from unauthorized copying, in the same way as DVDs.

Furthermore, studies have been conducted to apply DRM to BDs. When applying DRM to package media, content encrypted using a license key is recorded on a medium, whilst a license is separately delivered via a network. To play the content, the encrypted content recorded on the medium is decrypted using the license key.

According to DRM, encrypted content itself is copyable. For example, it is possible for one user to copy encrypted content which he or she acquired and recorded on an HDD to a CD-R or the like and hand it to another user. Even if the other user obtains the encrypted content, he or she cannot play back the content unless acquiring a license key. Such scheme is generally called superdistribution.

Superdistribution, however, is not necessarily accepted unconditionally for package media such as BDs.

A selling price of a package medium is usually several times or several tens of times of a selling price of a license in DRM content distribution. This is because users are expected to pay more for tangible products such as package media than intangible products such as licenses. Under such circumstances, content providers consider sales of package media as having primary importance, and therefore do not want even encrypted content to be copied freely. Allowing such acts could decrease sales in package media and eventually force the content providers to switch focus onto sales of licenses of lower prices.

In view of this, the present invention aims to provide a playback device and a playback method which can protect DRM encrypted content recorded on a recording medium from being unauthorizedly copied to another recording medium.

The stated aim can be achieved by a content playback device for decrypting encrypted content recorded on a recording medium and playing back the decrypted content, at least first-type encrypted content that is protected by a first protection method and second-type encrypted content that is protected by a second protection method different from the first protection method being recorded on the recording medium, and the encrypted content being any of the first-type encrypted content and the second-type encrypted content, the content playback device including:

a reception unit operable to receive a designation of the encrypted content; an acquisition unit operable to acquire protection method information showing one of the first and second protection methods that is used for protecting the encrypted content; a generation unit operable to generate a content key corresponding to the acquired protection method information; a decryption unit operable to read the encrypted content from the recording medium, and decrypt the encrypted content using the generated content key; and a playback unit operable to play back the decrypted content.

According to this construction, an appropriate content key can be generated to decrypt encrypted content, in the case where two pieces of encrypted content protected by different protection methods are recorded on the same recording medium.

Here, the first protection method may use a media key assigned to the recording medium, wherein the second protection method uses a license key assigned to a contract for use of the encrypted content, and the generation unit uses the media key to generate the content key if the protection method information shows the first protection method, and uses the license key to generate the content key if the protection method information shows the second protection method.



According to this construction, an appropriate content key can be generated depending on whether the encrypted content is protected by the first protection method using the media key or the second protection method using the license key.

Here, the recording medium may store the protection method information in correspondence with the encrypted content, wherein the acquisition unit acquires the protection method information by reading the protection method information from the recording medium.

According to this construction, the protection method information showing the protection method used for the encrypted content is stored on the recording medium. Accordingly, the protection method information can be reliably acquired by reading it from the recording medium.

Here, the content playback device may further include a judgment unit operable to acquire contract information relating to the contract, and judge, based on the acquired contract information, whether the encrypted content is permitted to be used, wherein the generation unit generates the content key if the encrypted content is judged as being permitted to be used.

According to this construction, the usability of the encrypted content is judged based on the acquired contract information, and the content key is generated if the

encrypted content is judged as being usable. This enables the encrypted content to be used in conformity with the contract for use of the encrypted content.

Here, the protection method information may include  
5 a content identifier for identifying the encrypted content and key type information showing a type of the content key, wherein the generation unit generates the content key which corresponds to the encrypted content identified by the content identifier and is of the type shown by the  
10 key type information.

According to this construction, the content key is generated so as to correspond to the encrypted content identified by the content identifier included in the protection method information and be of the type shown  
15 by the key type information included in the protection method information. Which is to say, an appropriate content key that corresponds to the encrypted content and the protection method used for the encrypted content can be generated.

20 Here, key type information showing a type of the content key may accompany the encrypted content on the recording medium, wherein the acquisition unit reads the key type information from the recording medium, and the generation unit generates the content key of the type shown  
25 by the read key type information.

According to this construction, the key type information accompanying the encrypted content is acquired to generate the content key of the type shown by the key type information. Which is to say, an appropriate content  
5 key that corresponds to the encrypted content and the protection method used for the encrypted content can be generated.

Here, the key type information may be multiplexed with the encrypted content on the recording medium, wherein  
10 the acquisition unit separates the key type information from the encrypted content.

According to this construction, the key type information multiplexed with the encrypted content is acquired by separating it from the encrypted content.  
15 Hence the key type information corresponding to the encrypted content can be acquired reliably.

Here, the protection method information may be stored on another recording medium, in correspondence with the encrypted content, wherein the acquisition unit acquires  
20 the protection method information by reading the protection method information from the other recording medium.

According to this construction, the protection method information adequately stored on the other recording medium can be acquired by reading it from the other recording  
25 medium.

Here, the acquisition unit may acquire the protection method information from another device that is connected to the content playback device via a network.

According to this construction, the protection  
5 method information which is adequately managed and protected by the other device can be acquired via the network.

Here, the recording medium may store media information showing the media key, wherein the generation  
10 unit uses the media key shown by the media information.

According to this construction, the media key is obtained from the media information stored on the recording medium. Hence the media key assigned to the recording medium can be obtained reliably.

15 Here, the media information may include the media key which has been encrypted using device information unique to the content playback device, wherein the generation unit reads the device information held in the content playback device, and decrypts the encrypted media  
20 key using the read device information to obtain the media key.

According to this construction, the encrypted media key is decrypted using the device information held in the content playback device. In this way, the media key  
25 assigned to the content playback device can be obtained

reliably.

Here, the recording medium may store a contract identifier for identifying contract information which relates to the contract and shows the license key, in  
5 correspondence with the encrypted content, wherein the generation unit reads the contract identifier from the recording medium, and uses the license key shown by the contract information identified by the read contract identifier.

10 According to this construction, the license key is identified by the contract identifier stored on the recording medium. Such a license key reliably corresponds to the encrypted content recorded on the recording medium.

Here, the recording medium may store a content  
15 identifier for identifying the encrypted content, wherein the generation unit reads the content identifier from the recording medium, and uses the license key corresponding to the content identifier.

According to this construction, the license key is  
20 associated with the content identifier stored on the recording medium. Such a license key reliably corresponds to the encrypted content recorded on the recording medium.

Here, the generation unit may include: a storage unit operable to store contract information including the  
25 license key, beforehand; and a generating unit operable

to read the contract information from the storage unit and generate the content key using the license key included in the read contract information, if the protection method information shows the second protection method.

5           According to this construction, the license key is included in the contract information stored in the storage unit. This enables the user to use the encrypted content with a simple operation.

          Here, contract information including the license key  
10   may be stored on another recording medium, in correspondence with the encrypted content, wherein the generation unit reads the contract information from the other recording medium, and uses the license key included in the read contract information.

15           According to this construction, the license key is stored on the other recording medium. Hence the use of the encrypted content can be limited to a user who has the other recording medium.

          Here, the content playback device may be connected,  
20   via a network, to a server device for delivering contract information including the license key, wherein the generation unit receives the contract information from the server device, and uses the license key included in the received contract information.

25           According to this construction, the license key which

is properly managed and protected by the server device can be obtained via the network.

Here, the recording medium may store content information unique to the encrypted content, in  
5 correspondence with the encrypted content, wherein the generation unit generates the content key using the media key and the content information, if the protection method information shows the first protection method.

According to this construction, the media key and  
10 the content information unique to the encrypted content are used if the protection method information shows the first protection method. As a result, a content key that depends on both the recording medium and the encrypted content can be obtained.

15 In the application of DRM to BDs, if both conventional copy-protected content and DRM content exist on a medium, a player cannot distinguish the two pieces of content. The DRM content cannot be decrypted using a media key. Likewise, the conventional copy-protected content cannot  
20 be decrypted using a license key, since there is no license for the conventional copy-protected content.

In view of this, the present invention aims to provide a data structure, in a recording medium on which both conventional copy-protected content and DRM content are  
25 recorded together, that is suitable for appropriately

playing both pieces of content. The present invention further aims to provide a recording medium on which data having the above data structure is recorded, and a playback device and a playback method for such a recording medium.

5

#### BRIEF DESCRIPTION OF DRAWINGS

FIG. 1 shows an overall construction of a content playback system which is an embodiment of the present invention.

10        FIG. 2 shows an internal construction of a playback device and information stored on a recording medium shown in FIG. 1.

FIG. 3 shows an example data structure of a playback path information table stored on the recording medium.

15        FIG. 4 shows an example of playback of video when the playback path information table shown in FIG. 3 is used.

FIG. 5 shows an example data structure of a button data table stored on the recording medium.

20        FIG. 6 shows an example of playback of video containing a plurality of buttons when the button data table shown in FIG. 5 is used.

FIG. 7 shows another example of playback of video containing a plurality of buttons when the button data  
25    table shown in FIG. 5 is used.



FIG. 8 shows an example data structure of a key control information table stored on the recording medium.

FIG. 9 shows an example data structure of a media information table stored on the recording medium.

5        FIG. 10 shows an example data structure of a rights information table stored in a rights storage unit in the playback device.

FIG. 11 shows an internal construction of a license server device shown in FIG. 1.

10       FIG. 12 is a flowchart of a content playback start operation by the playback device.

FIG. 13 is a flowchart of a media key generation operation by a media key generation unit in the playback device.

15       FIG. 14 is a flowchart of a content playback control operation by a playback control unit in the playback device.

FIG. 15 is a flowchart of a content decryption and playback operation by a decryption unit and a playback unit in the playback device.

20       FIG. 16 is a flowchart of a content key acquisition operation by a key control unit in the playback device.

FIG. 17 is a flowchart of a rights key acquisition operation by a rights management unit in the playback device.

25       FIG. 18 is a flowchart of a playability judgment

operation by the key control unit in the playback device.

FIG. 19 is a flowchart of a playability judgment operation by the rights management unit in the playback device.

5        FIG. 20 is a flowchart of an operation of acquiring rights information from the license server device by the playback device.

FIG. 21 shows an overall construction of a content recording/playback system which is a modification to the  
10    embodiment.

#### BEST MODE FOR CARRYING OUT THE INVENTION

The following describes a content playback system 1 which is an embodiment of the present invention.

##### 15    1.1. Construction of the Content Playback System 1

FIG. 1 shows a construction of the content playback system 1. As shown in the drawing, the content playback system 1 is roughly made up of a playback device 100 and a license server device 300 which are connected via an  
20    internet 10. A display device 113 such as a television monitor is connected with the playback device 100. Also, a recording medium 200 such as a BD is loaded to the playback device 100 by the user. The playback device 100 receives an operation from the user via a remote control 112.  
25    According to the received operation, the playback device

100 plays back content recorded on the recording medium 200, or acquires rights information relating to content from the license server device 300 and retains the acquired rights information.

5 1.2. Construction of the Recording Medium 200

FIG. 2 shows information stored on the recording medium 200. As illustrated, the recording medium 200 stores a playback path information table 210, encrypted content 231, 232, ... , 238, a key control information table 260, and a media information table 280, in advance. The playback path information table 210, the encrypted content 231, 232, ... , 238, the key control information table 260, and the media information table 280 constitute composite content (compound content). The composite content referred to here is a type of content that includes a combination of different pieces of content.

(1) Playback Path Information Table 210

FIG. 3 shows an example of the playback path information table 210. In the drawing, the playback path information table 210 includes eight sets of playback control information 291, 292, ... , 298, which each correspond to any of the encrypted content 231, 232, ... , 238 recorded on the recording medium 200. These eight sets of playback control information 291, 292, ... , 298 define an order in which the encrypted content 231, 232, ... , 238 are decrypted

and played back. Each set of playback control information includes a playback number, a content name, a next playback number, and an alternative playback number. Here, the playback control information may not include the  
5 alternative playback number, and further may not include the next playback number.

(Playback Number)

The playback number included in the playback control information is an index number for uniquely identifying  
10 the playback control information. The playback number begins with 1, and is incremented by 1 for each set of playback control information. For example, the playback control information 291 has a playback number 212 "1", which uniquely identifies the playback control information  
15 291. Meanwhile, the playback control information 292 includes a playback number 217 "2", which uniquely identifies the playback control information 292.

(Content Name)

The content name included in the playback control  
20 information identifies encrypted content corresponding to the playback control information. As one example, the content name is a filename for uniquely identifying the encrypted content that is recorded on the recording medium  
200 as one file.

25 (Next Playback Number)

The next playback number included in the playback control information designates playback control information corresponding to encrypted content that is to be decrypted and played next, when the decryption and playback of the encrypted content corresponding to the former playback control information have completed. The next playback number is not set if there is no encrypted content to be decrypted and played next.

For instance, the playback control information 291 has a next playback number 214 "2". Accordingly, after the decryption and playback of the encrypted content identified by a content name 213 "Opening.mpg" have completed, encrypted content corresponding to the playback control information 292 designated by the next playback number 214 "2", i.e. the encrypted content identified by a content name 218 "Trailer.mpg", is decrypted and played. (Alternative Playback Number)

The alternative playback number included in the playback control information designates playback control information corresponding to encrypted content that is to be decrypted and played alternatively if the decryption and playback of the encrypted content designated by the next playback number are not permitted.

For instance, the playback control information 292 has a next playback number 219 "3" and an alternative

5 playback number 220 "4". Suppose the decryption and playback of encrypted content corresponding to the playback control information 293 designated by the next playback number 219 "3", i.e. encrypted content identified by a content name 221 "Movie.mpg", are not permitted. In this case, after the decryption and playback of the encrypted content identified by the content name 218 "Trailer.mpg" have completed, encrypted content corresponding to the playback control information 294 designated by the  
10 alternative playback number 220 "4", i.e. encrypted content identified by a content name 222 "Warning.mpg", is decrypted and played.

If the playback control information includes no alternative playback number, the decryption and playback  
15 of the encrypted content designated by the next playback number are carried out irrespective of whether that encrypted content is playable or not.

(Playback Example)

FIG. 4 shows an example of playback when the playback  
20 path information table 210 shown in FIG. 3 is used.

As shown in FIG. 4, video 401 is played first, and then video 402 is played. After this, video 403 is played if playable, and then video 405 is played. If video 403 is unplayable, video 404 is played instead. Also, video  
25 406, 407, and 408 are played depending on conditions.

Here, video 401, 402, ... , 408 respectively correspond to the playback control information 291, 292, ... , 298 shown in FIG. 3.

(2) Encrypted Content 231, 232, ... , 238

5       The encrypted content 231, 232, ... , 238 each constitute one file on the recording medium 200.

      The encrypted content 231, 232, ... , 238 have the same data structure. Which is to say, the encrypted content is obtained by applying an encryption algorithm to a payload  
10 of each packet of a transport stream, excluding an adaptation field, that is generated by multiplexing an MPEG-2 video elementary stream and an MPEG-2 audio elementary stream according to an MPEG-2 multiplexing system. The encryption algorithm referred to here is AES  
15 (Advanced Encryption Standard) as one example, though other secret-key encryption algorithms are applicable too.  
(Button Data Table 240)

      If the encrypted content is menu display content, the encrypted content includes, in encrypted form, a button  
20 data table 240 for displaying buttons as a private stream, in addition to the video elementary stream and the audio elementary stream. It should be noted here that the manner in which the encrypted button data table is included is not limited to this.

25       FIG. 5 shows an example of the button data table 240.

In the drawing, the button data table 240 includes four sets of button data, which respectively correspond to four buttons 422, 423, 424, and 425 in a menu display 421 shown in FIG. 6, and also respectively correspond to four buttons  
5 432, 433, 434, and 435 in a menu display 431 shown in FIG.

7. Each set of button data includes a button number, a playback number, an upper button number, a lower button number, a left button number, a right button number, unselected data, selected data, and grayed-out data. Here,  
10 the button data may not include the grayed-out data.

(a) Button Number

The button number included in the button data is an index number for uniquely identifying the button data. The button number begins with 1, and is incremented by  
15 1 for each set of button data. When the playback of the menu display content starts, a button corresponding to button data identified by a button number 241 "1" is put in a selected state.

(b) Playback Number

20 The playback number included in the button data identifies playback control information corresponding to encrypted content that is to be played when selection of a button corresponding to the button data is confirmed via the remote control 112.

25 For example, the button data identified by the button



number 241 "1" has a playback number 242 "2". Accordingly, when a confirmation operation is made via the remote control 112 while the button corresponding to this button data is in a selected state, the encrypted content corresponding to the playback control information 292 that has the playback number 217 "2" in the playback path information table 210 in FIG. 3, i.e. the encrypted content identified by the content name 218 "Trailer.mpg", is decrypted and played.

10 (c) Upper Button Number

The upper button number included in the button data identifies button data corresponding to a button that is put into a selected state when an up movement operation is made via the remote control 112 while the button corresponding to the former button data is in a selected state.

For instance, the button data identified by the button number 241 "1" has an upper button number 243 "4". This being so, if an up movement operation is made via the remote control 112 while the button corresponding to this button data is in a selected state, a button corresponding to button data identified by the upper button number 243 "4" is put into a selected state.

(d) Lower Button Number

25 The lower button number included in the button data

identifies button data corresponding to a button that is put into a selected state when a down movement operation is made via the remote control 112 while the button corresponding to the former button data is in a selected state.

(e) Left Button Number

The left button number included in the button data identifies button data corresponding to a button that is put into a selected state when a left movement operation is made via the remote control 112 while the button corresponding to the former button data is in a selected state.

(f) Right Button Number

The right button number included in the button data identifies button data corresponding to a button that is put into a selected state when a right movement operation is made via the remote control 112 while the button corresponding to the former button data is in a selected state.

(g) Unselected Data

The unselected data included in the button data is image data showing the button to be displayed when the button is in an unselected state.

(h) Selected Data

The selected data included in the button data is image

data showing the button to be displayed when the button is in a selected state.

(i) Grayed-out Data

The grayed-out data included in the button data is image data showing the button to be displayed when the button is in a grayed-out state, i.e., an unselectable state. This image data is created, for example, by replacing the alternate pixels of the unselected data with blank pixels. Such image data is less distinct than the unselected data, thereby indicating that the button cannot be selected. The grayed-out state is explained in more detail later.

(3) Key Control Information Table 260

FIG. 8 shows an example of the key control information table 260. As illustrated, the key control information table 260 includes a plurality of sets of key control information, which each correspond to any of the encrypted content 231, 232, ... , 238 recorded on the recording medium 200. Each set of key control information includes a content name, content information, key generation information, playability information, copyability information, and rights mode information.

(Content Name)

The content name included in the key control information identifies encrypted content corresponding

to the key control information. Like the content name in the playback path information table 210 shown in FIG. 3, the content name in the key control information table 260 shows a filename that identifies the corresponding encrypted content. Unlike the playback path information table 210, however, the same content name never appears more than once in the key control information table 260. (Content Information)

The content information included in the key control information is used to generate a content key for decrypting the encrypted content corresponding to the key control information. The content information is unique to the corresponding encrypted content. (Key Generation Information)

The key generation information included in the key control information specifies a method of generating the content key for the encrypted content corresponding to the key control information. The key generation information takes one of the values "00", "01", and "10". The value "00" indicates the content key is to be generated using a media key. The value "01" indicates the content key is to be generated using a composite key. The value "10" indicates the content key is to be generated using a rights key (also referred to as a license key). The media key, the composite key, and the rights key are explained

in detail later.

(Playability Information)

The playability information included in the key control information shows whether the encrypted content corresponding to the key control information is playable or not. The playability information takes one of the values "1" and "0". The value "1" indicates the encrypted content is playable. The value "0" indicates the encrypted content is unplayable.

10 Although the playability information shows whether the encrypted content is playable or not in this example, this is not a limit for the present invention. For example, the playability information may show a playback quality, such that the encrypted content is judged as being  
15 unplayable if the playability information shows a high playback quality, and playable if the playability information shows a low playback quality.

(Copyability Information)

The copyability information included in the key control information shows whether the encrypted content corresponding to the key control information is copyable or not. The copyability information takes one of the values "01", "10", and "00". The value "01" indicates "Once", i.e. the content can be copied one generation. The value  
25 "10" indicates "Free", i.e. the content can be copied freely.

The value "00" indicates "Never", i.e., the content is never to be copied.

Although the copyability information shows any of "Once", "Free", and "Never" in this example, the present invention is not limited to this. For example, the copyability information may show a copy quality. Also, the copyability information may contain information for specifying copy destination media.

(Rights Mode Information)

The rights mode information included in the key control information specifies one or more rights modes specified for the encrypted content corresponding to the key control information, when the key generation information in the key control information is "10" (rights key) or "01" (composite key). For instance, when the rights mode information is "01", mode A is specified for the content. When the rights mode information is "10", mode B is specified for the content. When the rights mode information is "01,10", modes A and B are specified for the content.

A rights mode mentioned here is a mode of generating rights for the content. As one example, mode A generates the rights based on a maximum number of times the playback of the content is permitted, whilst mode B generates the rights based on an expiration date until which the playback of the content is permitted.

When the key generation information in the key control information is "00" (media key), the rights mode information in the key control information is "00", indicating that no rights mode is specified.

5           In FIG. 8, for example, rights mode information 266 is "00", which means no rights mode is specified for content corresponding to key control information that includes the rights mode information 266.

10           Meanwhile, rights mode information 272 is "01", which means mode A is specified for content corresponding to key control information that includes the rights mode information 272. Accordingly, only rights that are generated in mode A are used as the rights for use of the content.

15           Also, rights mode information 273 is "01,10", which means modes A and B are specified for content corresponding to key control information that includes the rights mode information 273. Accordingly, rights that are generated in any of modes A and B are used as the rights for use  
20 of the content.

          Further, rights mode information 274 is "10", which means mode B is specified for content corresponding to key control information that includes the rights mode information 274. Accordingly, only rights that are  
25 generated in mode B are used as the rights for use of the

content.

(4) Media Information Table 280

FIG. 9 shows an example of the media information table 280. As illustrated, the media information table 280 includes a plurality of sets of media information, which each correspond to an individual playback device. Each set of media information includes device information and an encrypted media key.

(Device Information)

10 The device information included in the media information is uniquely given to a playback device corresponding to the media information.

(Encrypted Media key)

15 The encrypted media key included in the media information is generated by applying an encryption algorithm to a media key using a device key unique to the playback device corresponding to the media information. The encryption algorithm referred to here is AES as one example, though other secret-key encryption algorithms are equally applicable. The media key is uniquely assigned to the recording medium 200.

Thus, the media information table 280 contains encrypted media keys generated for separate playback devices. Suppose one playback device becomes  
25 unauthorized as a result of hacking or the like. In such



a case, in the subsequent production of recording media a media information table that does not include media information corresponding to the unauthorized playback device is created and written to each recording medium.

5 In so doing, playback of content by unauthorized devices can be prevented.

In this embodiment, the sets of media information as many as the playback devices are stored in the media information table 280. This unnecessarily increases a data size of the media information table 280. To avoid this, the data size of the media information table 280 may be reduced using a binary tree.

### 1.3. Construction of the Playback Device 100

FIG. 2 also shows a construction of the playback device 100. In the drawing, the playback device 100 includes a drive unit 101, a playback control unit 102, a decryption unit 103, a key control unit 104, a media key generation unit 105, a reception unit 106, a playback unit 107, a rights management unit 108, a rights storage unit 109, a communication unit 110, a device information storage unit 111, and a power supply unit (not illustrated) for supplying power to each construction element of the playback device 100.

The playback device 100 is actually realized by a computer system that is roughly made up of a CPU, a working

memory, a flash memory, a BD drive, a video adapter, a network adapter, and the like. The drive unit 101 is realized by the BD drive. The reception unit 106 receives an operation from the remote control 112 via an infrared signal. The playback unit 107 is realized by the video adapter. The rights storage unit 109 and the device information storage unit 111 are realized by the flash memory. The communication unit 110 is realized by the network adapter. Also, the flash memory stores a plurality of computer programs showing operations of the playback control unit 102, the decryption unit 103, the key control unit 104, the media key generation unit 105, and the rights management unit 108. Functions of the playback control unit 102, the decryption unit 103, the key control unit 104, the media key generation unit 105, and the rights management unit 108 are achieved by the CPU operating in accordance with the corresponding computer programs.

(1) Device Information Storage Unit 111 and Rights Storage Unit 109

(Device Information Storage Unit 111)

The device information storage unit 111 stores device information 141 and a device key 142 beforehand, as shown in FIG. 2.

The device information 141 is uniquely given to the playback device 100. The device key 142 is uniquely given

to the playback device 100.

(Rights Storage Unit 109)

The rights storage unit 109 stores a rights information table 121 beforehand, as shown in FIG. 2.

5        FIG. 10 shows an example of the rights information table 121. In the drawing, the rights information table 121 includes a plurality of sets of rights information, which each correspond to any of the encrypted content 231, 232, ... , 238, and show rights to play back the corresponding  
10    content.

Each set of rights information is made up of rights mode information, a content name, a rights key, a playback count, and a playback expiration date. Here, the rights information may not include the playback count or the  
15    playback expiration date.

The rights mode information included in the rights information shows a rights mode specified for the encrypted content corresponding to the rights information. The rights mode represents a method of generating rights for  
20    use of the content.

The content name included in the rights information identifies the encrypted content corresponding to the rights information. Like the content name included in the playback path information table 210 shown in FIG. 3, the  
25    content name in the rights information table 121 is a

filename that uniquely identifies the corresponding content.

The rights key included in the rights information is key information given to the rights shown by the rights  
5 information.

The playback count included in the rights information is a maximum number of times the playback of the corresponding content is permitted. The absence of the playback count in the rights information means the content  
10 can be played back an unlimited number of times.

The playback expiration date included in the rights information shows an expiration date until which the playback of the corresponding content is permitted. The absence of the playback expiration date in the rights  
15 information means the content can be played back without a time limit.

Though the rights information is made up of the five items, i.e. the rights mode information, the content name, the rights key, the playback count, and the playback  
20 expiration date in the above example, the present invention is not limited to this. For instance, the rights information may include other items such as a playback device limitation, a user limitation, and a geographical area limitation.

25 (2) Playback Control Unit 102

The playback control unit 102 receives an instruction to play back content recorded on the recording medium 200, from the reception unit 106. The playback control unit 102 also receives a signal indicating detection of  
5 insertion of the recording medium 200, from the drive unit 101.

Upon receiving the playback instruction from the reception unit 106 or the detection signal from the drive unit 101 immediately after receiving power from the power  
10 supply unit, the playback control unit 102 outputs an instruction to decrypt the content recorded on the recording medium 200, to the decryption unit 103.

After this, the playback control unit 102 receives decryption failure notification indicating that the  
15 content decryption has failed or media key acquisition success notification indicating that media key acquisition has succeeded, from the decryption unit 103. Upon receiving the decryption failure notification, the playback control unit 102 terminates the subsequent  
20 playback control operation. Upon receiving the media key acquisition success notification, the playback control unit 102 performs the playback control operation as follows.

(Playback Control Operation)

25 The playback control unit 102 has the drive unit 101

read playback control information having the playback number "1" from the playback path information table 210 on the recording medium 200. The playback control unit 102 extracts a content name from the read playback control information, and outputs the extracted content name to the decryption unit 103. The playback control unit 102 instructs the decryption unit 103 to decrypt and play encrypted content identified by the content name.

Once the decryption and playback of the encrypted content identified by the content name have completed, the playback control unit 102 attempts to extract a next playback number from the playback control information. If there is no next playback number in the playback control information, the playback control unit 102 ends the playback control operation.

If there is a next playback number in the playback control information, the playback control unit 102 has the drive unit 101 read playback control information whose playback number matches the extracted next playback number from the playback path information table 210. The playback control unit 102 then extracts a content name from the read playback control information, and outputs the extracted content name to the rights management unit 108 via the decryption unit 103 and the key control unit 104. The playback control unit 102 inquires of the rights

management unit 108 whether encrypted content identified by the content name is playable or not, via the decryption unit 103 and the key control unit 104.

If the rights management unit 108 replies that the  
5 content is unplayable, the playback control unit 102 extracts an alternative playback number from the playback control information. The playback control unit 102 has the drive unit 101 read playback control information whose playback number matches the extracted alternative playback  
10 number from the playback path information table 210. The playback control unit 102 then extracts a content name from the read playback control information, outputs the extracted content name to the decryption unit 103, and instructs the decryption unit 103 to decrypt and play  
15 encrypted content identified by the content name. Once the decryption and playback of the encrypted content have completed, the playback control unit 102 attempts to extract a next playback number from the playback control information. If no next playback number is included in  
20 the playback control information, the playback control unit 102 ends the playback control operation.

If the rights management unit 108 replies that the content is playable, on the other hand, the playback control unit 102 outputs the content name to the decryption unit  
25 103, and instructs the decryption unit 103 to decrypt and

play the encrypted content identified by the content name.  
Once the decryption and playback of the encrypted content  
have completed, the playback control unit 102 attempts  
to extract a next playback number from the playback control  
5 information. If the playback control information has no  
next playback number, the playback control unit 102 ends  
the playback control operation.

If the playback control information has a next  
playback number, the playback control unit 102 repeats  
10 the above operation until no next playback number is  
extracted.

(3) Decryption Unit 103, Playback Unit 107, and Display  
Device 113  
(Decryption Unit 103)

15 The decryption unit 103 receives an instruction to  
decrypt the content recorded on the recording medium 200  
from the playback control unit 102, and outputs an  
instruction to acquire a media key to the key control unit  
104.

20 After this, the decryption unit 103 receives media  
key acquisition failure notification indicating that the  
media key acquisition has failed or media key acquisition  
success notification indicating that the media key  
acquisition has succeeded, from the key control unit 104.

25 Upon receiving the media key acquisition failure



notification, the decryption unit 103 outputs decryption failure notification indicating that the content decryption has failed, to the playback control unit 102.

Upon receiving the media key acquisition success notification, the decryption unit 103 outputs the media key acquisition success notification to the playback control unit 102.

The decryption unit 103 then receives a content name and an instruction to decrypt encrypted content identified by the content name, from the playback control unit 102. The decryption unit 103 has the key control unit 104 acquire a content key corresponding to the encrypted content, and has the drive unit 101 read the encrypted content from the recording medium 200.

If the decryption unit 103 receives content key acquisition failure notification indicating that the content key acquisition has failed from the key control unit 104, the decryption unit 103 outputs decryption failure notification indicating that the content decryption has failed to the playback control unit 102, and terminates the subsequent operation.

Next, the decryption unit 103 judges whether the read encrypted content contains an encrypted button data table. This judgment can be made by checking whether the encrypted content contains a private stream with reference to an

unencrypted PAT (Program Association Table) or PMT (Program Map Table) in the encrypted content, though this is not a limit for the present invention.

(a) If the encrypted content does not contain an encrypted button data table, the decryption unit 103  
5 decrypts the encrypted content in units of packets using the content key, and outputs the decrypted content to the playback unit 107.

(b) If the encrypted content contains an encrypted  
10 button data table, the decryption unit 103 decrypts the encrypted button data table using the content key, and performs the following process (i) to (iv) on each set of button data in the decrypted button data table.

(i) The decryption unit 103 extracts a playback number  
15 from the button data.

(ii) The decryption unit 103 acquires a content name corresponding to the extracted playback number from the playback path information table 210, via the drive unit 101. In detail, the decryption unit 103 has the drive unit  
20 101 read playback control information whose playback number matches the extracted playback number from the playback path information table 210 on the recording medium 200, and extracts a content name from the read playback control information.

25 (iii) The decryption unit 103 outputs the content

name to the rights management unit 108 via the key control unit 104, and inquires of the rights management unit 108 whether content identified by the content name is playable or not, via the key control unit 104.

5           (iv) If the rights management unit 108 replies that the content is playable, the decryption unit 103 extracts unselected data and selected data that represent normal button display, from the button data. If the rights management unit 108 replies that the content is unplayable,  
10 the decryption unit 103 extracts grayed-out data that represents grayed-out button display, from the button data. This completes the process (i) to (iv).

The decryption unit 103 then decrypts the encrypted content in units of packets using the content key, and  
15 outputs the decrypted content to the playback unit 107.

The decryption unit 103 also outputs the selected data and unselected data or the grayed-out data extracted for each set of button data, to the playback unit 107.  
(Playback Unit 107)

20           The playback unit 107 receives decrypted content from the decryption unit 103, and decodes it to generate digital video and audio data. The playback unit 107 generates analog video and audio signals from the digital video and audio data, and outputs the analog video and audio signals  
25 to the display device 113.

Also, the playback unit 107 receives selected data and unselected data or grayed-out data extracted for each set of button data from the decryption unit 103, and overlays the selected data and unselected data or the grayed-out data on the video data to display each button. In this way, the display state of each button is varied depending on playability of content corresponding to the button. Which is to say, the button is displayed in a normal state if the content is playable, and in a grayed-out state if the content is unplayable. When the button is grayed out, it is impossible to confirm the selection of the button. (Display Device 113)

The display device 113 receives analog video and audio signals from the playback unit 107, and outputs the video signal as video and the audio signal as sounds.

#### (4) Key Control Unit 104

The key control unit 104 receives an instruction to acquire a media key from the decryption unit 103, and outputs an instruction to generate the media key to the media key generation unit 105.

Following this, the key control unit 104 receives either a decrypted media key or media key generation failure notification indicating that the media key generation has failed, from the media key generation unit 105.

Upon receiving the media key generation failure

notification, the key control unit 104 outputs media key acquisition failure notification indicating that the media key acquisition has failed, to the decryption unit 103.

Upon receiving the decrypted media key, the key control unit 104 outputs media key acquisition success notification indicating that the media key acquisition has succeeded, to the decryption unit 103.

(Content Key Acquisition)

The key control unit 104 then acquires a content key in the following manner, according to an instruction from the decryption unit 103.

The key control unit 104 receives a content name and a content key acquisition instruction from the decryption unit 103. The key control unit 104 has the drive unit 101 read key control information having the received content name from the key control information table 260 on the recording medium 200, and extracts key generation information from the read key control information.

The key control unit 104 judges whether the key generation information is "00" which indicates "media key". If the key generation information is "00", the key control unit 104 extracts content information from the key control information, and concatenates the decrypted media key received from the media key generation unit 105 and the extracted content information in this order. The key

control unit 104 then applies a one-way function to the concatenation outcome, to thereby generate the content key. The one-way function referred to here is SHA-1 as one example.

```

5      (content key) = SHA-1 ((decrypted media key) ||
                                (content information))

```

Here, "SHA-1 (X)" denotes a hash value obtained by converting X by SHA-1, and "A || B" denotes an outcome of concatenating A and B in this order.

10           It should be noted here that the generation of the  
content key is not limited to the above. For example, other  
hash functions or one-way functions may be used.  
Alternatively, the content key may be generated by  
decrypting the content information using the decrypted  
15 media key.

The key control unit 104 outputs the generated content key to the decryption unit 103.

If the key generation information is not "00", the key control unit 104 extracts rights mode information from the key control information, and outputs the content name and the rights mode information to the rights management unit 108. The key control unit 104 controls the rights management unit 108 to acquire a rights key corresponding to content identified by the content name. If the key control unit 104 receives rights key acquisition failure

notification indicating that the rights key acquisition has failed from the rights management unit 108, the key control unit 104 outputs content key acquisition failure notification indicating that the content key acquisition  
5 has failed to the decryption unit 103, and ends the subsequent operation.

Next, the key control unit 104 judges whether the key generation information is "01" or "10". If the key generation information is "10" which indicates "rights  
10 key", the key control unit 104 sets the acquired rights key as the content key, and outputs the content key to the decryption unit 103.

Though the rights key itself is set as the content key if the key generation information indicates "rights  
15 key" in the above example, the present invention is not limited to such. For instance, the content key may be generated from the rights key and the content information using a one-way function. Also, the generation of the content key from the rights key may be performed not by  
20 the key control unit 104 but by the rights management unit 108. This enhances security especially when the key control unit 104 and the rights management unit 108 are implemented as separate tamper-resistant modules, because the rights key need not be output to the key control unit  
25 104.

If the key generation information is "01" which indicates "composite key", the key control unit 104 concatenates the decrypted media key and the acquired rights key in this order, and performs a one-way function  
5 on the concatenation outcome to generate the content key.

$$(\text{content key}) = \text{SHA-1} ((\text{decrypted media key}) \parallel (\text{rights key}))$$

The key control unit 104 outputs the generated content key to the decryption unit 103.

10 Note here that the generation of the content key is not limited to the use of a one-way function. For instance, the content key may be generated by decrypting the content information using the decrypted media key, or by decrypting the rights key in encrypted form using the decrypted media  
15 key. The content information may be used in the generation of the content key. Especially when the key control unit 104 and the rights management unit 108 are implemented as separate tamper-resistant modules, the key control unit 104 may generate information from the decrypted media key  
20 and the content information and notify it to the rights management unit 108, which then generates the content key from the notified information and the rights key. This makes it unnecessary to output the decrypted media key to the rights management unit 108 and the rights key to  
25 the key control unit 104, which contributes to higher



security.

(Content Playability Judgment)

When playability of content needs to be judged during the playback control operation, the key control unit 104  
5 reads key control information corresponding to the content from the recording medium 200 and judges the playability of the content, in the following way.

The key control unit 104 receives a content name and an instruction to judge playability of content identified  
10 by the content name, from the decryption unit 103. In response, the key control unit 104 has the drive unit 101 read key control information having the received content name from the key control information table 260 on the recording medium 200, and extracts key generation  
15 information from the read key control information.

The key control unit 104 judges whether the key generation information is "00" which indicates "media key". If the key generation information is "00", the key control unit 104 extracts playability information from the key  
20 control information, and judges whether the playability information is "0" or "1". If the playability information is "1", the key control unit 104 outputs playback permission notification indicating that the content is playable, to the decryption unit 103. If the playability information  
25 is "0", the key control unit 104 outputs playback

prohibition information indicating that the content is unplayable, to the decryption unit 103.

If the key generation information is not "00", the key control unit 104 extracts the playability information from the key control information, and judges whether the playability information is "0" or "1". If the playability information is "1", the key control unit 104 outputs playback permission notification to the decryption unit 103. If the playability information is "0", the key control unit 104 extracts rights mode information from the key control information, and outputs the rights mode information, the content name, and a rights judgment instruction to the rights management unit 108. The key control unit 104 then receives a judgment result on the playability of the content from the rights management unit 108, and outputs the judgment result to the decryption unit 103.

In the case where the key generation information is not "00", even when the content is judged as being playable, the content key cannot be obtained and therefore the content cannot be decrypted and played unless the rights management unit 108 acquires the rights key. To avoid any confusion resulting from this, it is more preferable to judge the content as being playable after confirming the presence of the rights key, than to judge the content as being playable

simply based on the playability information.

(5) Media key Generation Unit 105

The media key generation unit 105 receives a media key generation instruction from the key control unit 104.

5 In response, the media key generation unit 105 reads the device information 141 from the device information storage unit 111. The media key generation unit 105 have the drive unit 101 read media information from the media information table 280 on the recording medium 200, and extracts device  
10 information from the read media information. The media key generation unit 105 compares the extracted device information with the device information 141.

If the extracted device information does not match the device information 141, the media key generation unit  
15 105 repeats the reading of next media information from the media information table 280, the extraction of device information from the read media information, and the comparison, until every set of media information has been read from the media information table 280.

20 If the same device information as the device information 141 is not found in the media information table 280, the media key generation unit 105 outputs media key generation failure notification indicating that the media key generation has failed, to the key control unit 104.

25 If the extracted device information matches the

device information 141, on the other hand, the media key generation unit 105 reads the device key 142 from the device information storage unit 111, and extracts an encrypted media key from the read media information. The media key generation unit 105 decrypts the encrypted media key using the device key 142 according to AES, and outputs the decrypted media key to the key control unit 104.

(6) Rights Management Unit 108

(Rights Key Acquisition)

10       The rights management unit 108 receives a content name and rights mode information from the key control unit 104. The rights management unit 108 judges whether the rights mode information is "00", "01", "10", or "01,10", to judge whether any rights mode is specified for content  
15 identified by the content name.

      If a rights mode is specified for the content, that is, if the rights mode information is "01", "10", or "01,10", the rights management unit 108 attempts to extract rights information having both the received rights mode  
20 information and content name, from the rights information table 121 in the rights storage unit 109.

      In more detail, if the rights mode information is "01", the rights management unit 108 attempts to extract rights information having both the rights mode information  
25 "01" and the content name. If the rights mode information

is "10", the rights management unit 108 attempts to extract rights information having both the rights mode information "10" and the content name. If the rights mode information is "01,10", the rights management unit 108 attempts to  
5 extract rights information having both the rights mode information "01" and the content name, and rights information having both the rights mode information "10" and the content name.

Suppose the rights mode information specifies mode  
10 A and the content name is "Making.mpg". In this case, rights information 132, and not rights information 133, is extracted from the rights information table 121 shown in FIG. 10. Suppose the rights mode information specifies modes A and B and the content name is "Making.mpg". In  
15 this case, the rights information 132 and the rights information 133 are extracted from the rights information table 121.

If no rights mode is specified for the content, that is, if the rights mode information is "00", the rights  
20 management unit 108 attempts to extract rights information having the content name from the rights information table 121.

For instance, if the rights mode information specifies no rights mode and the content name is "Movie.mpg",  
25 rights information 131 is extracted from the rights

information table 121 shown in FIG. 10.

As a result, either at least one set of rights information is extracted, or no set of rights information is extracted at all.

5           In this embodiment, playback of content is instructed after judging the playability of the content. Accordingly, the failure to extract rights information means the occurrence of some kind of problem such as an unauthorized attack.

10           If a plurality of sets of rights information are extracted, the rights management unit 108 selects one of the sets of rights information. If one set of rights information is extracted, the rights management unit 108 selects that rights information. The rights management  
15 unit 108 then judges whether the content identified by the content name is playable, using a playback count and/or a playback expiration date included in the selected rights information.

          When using the playback count, the rights management  
20 unit 108 judges the content as being playable if the playback count is not "0", and unplayable if the playback count is "0".

          When using the playback expiration date, the rights management unit 108 judges the content as being playable  
25 if a current time shown by a clock equipped in the rights

management unit 108 is within the playback expiration date, and unplayable if the current time exceeds the playback expiration date.

When using both the playback count and the playback expiration date, the rights management unit 108 judges the content as being playable if both of the above judgments are affirmative, and unplayable if any of the above judgments is negative.

If the content is judged as being playable, the rights management unit 108 extracts a rights key from the selected rights information, and outputs the rights key to the key control unit 104.

If the content is judged as being unplayable, it means the rights key acquisition has failed, as in the case where no set of rights information is extracted. When this happens, the rights management unit 108 outputs rights key acquisition failure notification indicating that the rights key acquisition has failed, to the key control unit 104.

#### (Content Playability Judgment)

The rights management unit 108 receives a rights judgment instruction, a content name, and rights mode information from the key control unit 104. The rights management unit 108 then judges whether the rights mode information is "00", "01", "10", or "01,10", to judge

whether any rights mode is specified for content identified by the content name, in the same way as above.

If a rights mode is specified for the content, the rights management unit 108 attempts to extract rights information having both the received rights mode  
5 information and content name from the rights information table 121 in the rights storage unit 109, in the same way as above.

If no rights mode is specified for the content, the  
10 rights management unit 108 attempts to extract rights information having the received content name from the rights information table 121, in the same way as above.

As a result, either at least one set of rights information is extracted, or no set of rights information  
15 is extracted.

If at least one set of rights information is extracted, the rights management unit 108 selects one set of rights information, and judges whether the content is playable based on a playback count and/or a playback expiration  
20 date included in the selected rights information, in the same way as above.

If the content is judged as being playable as a result, the rights management unit 108 outputs a judgment result indicating that the content is playable, to the key control  
25 unit 104.



If the content is judged as being unplayable, the rights management unit 108 outputs a judgment result indicating that the content is unplayable, to the key control unit 104.

5        If no set of rights information is extracted, the rights management unit 108 outputs a judgment result indicating that the content is unplayable, to the key control unit 104.

(7) Remote Control 112, Reception Unit 106, Drive Unit  
10   101, and Communication Unit 110  
(Remote Control 112)

The remote control 112 has an enclosure that is formed by an upper case and a lower case, as shown in FIG. 1. In the enclosure, a flat wiring board is held by the lower  
15   case. Also, a plurality of operation buttons are provided on the upper case. These operation buttons are engraved with such legends that indicates activation, confirmation, playback, the numerals 1 to 12, and up, down, left, and right movements.

20        Switches which are opened and closed according to the user's button operations are disposed on the wiring board at the positions corresponding to the operation buttons. Furthermore, an infrared radiation unit and a conversion circuit are formed on the wiring board.

25        When a switch is opened or closed as a result of the

user's operation on a corresponding button, the conversion circuit detects the opening or closing of the switch, generates an electrical signal corresponding to the opening or closing of the switch, converts the electrical signal to a digital signal, and outputs the digital signal to the infrared radiation unit. The infrared radiation unit receives the digital signal, and emits or stops an infrared ray depending on the digital signal.

In so doing, the remote control 112 radiates an infrared ray carrying a signal corresponding to the user's button operation.

(Reception Unit 106)

The reception unit 106 receives an infrared ray from the remote control 112, extracts a signal corresponding to a button operation from the infrared ray, and outputs the extracted signal to the playback control unit 102.

For example, if the extracted signal shows a playback operation, the reception unit 106 outputs a playback instruction to the playback control unit 102.

(Communication Unit 110)

The communication unit 110 is connected to the license server device 300 via the internet 10.

To acquire rights, the communication unit 110 establishes an encrypted channel, such as a SAC (Secure Authentication Channel), with a communication unit 301

in the license server device 300. In detail, the communication unit 110 shares a session key with the license server device 300. The communication unit 110 then requests transmission of rights from the license server device 300. The communication unit 110 receives encrypted rights information from the communication unit 301 in response, decrypts the encrypted rights information using the session key, and writes the decrypted rights information to the rights information table 121 in the rights storage unit 109.

(Drive Unit 101)

The drive unit 101 reads information from the recording medium 200, under control of any of the playback control unit 102, the decryption unit 103, the key control unit 104, and the media key generation unit 105. The drive unit 101 outputs the read information to the corresponding unit.

#### 1.4. Construction of the License Server Device 300

FIG. 11 shows a construction of the license server device 300. In the drawing, the license server device 300 includes the communication unit 301, a communication control unit 302, a rights generation unit 303, and a control unit 306. A display unit 304 and an input unit 305 are connected to the license server device 300.

The license server device 300 is actually realized

by a computer system that includes a microprocessor, a ROM, a RAM, a hard disk unit, a communication unit (network adapter), a display unit, a keyboard, and a mouse. A computer program is stored on the RAM or the hard disk  
5 unit. Functions of the construction elements of the license server device 300 are achieved by the microprocessor operating in accordance with this computer program.

The communication unit 301 is connected to the  
10 playback device 100 via the internet 10. The communication unit 301 establishes an encrypted channel such as a SAC with the communication unit 110 in the playback device 100, under control of the communication control unit 302. To do so, the communication unit 301 shares a session key  
15 with the playback device 100. After establishing the encrypted channel, the communication unit 301 transfers information between the rights generation unit 303 and the playback device 100, under control of the communication control unit 302.

20 The rights generation unit 303 receives a request for transmission of rights from the playback device 100 via the internet 10, the communication unit 301, and the communication control unit 302, after the establishment of the encrypted channel. The rights generation unit 303  
25 responsively generates rights information for the playback

device 100, encrypts the rights information using the session key, and transmits the encrypted rights information to the playback device 100 via the communication control unit 302, the communication unit 301, and the internet  
5 10.

The input unit 305 receives an operation from the operator of the license server device 300, and outputs the received operation to the control unit 306.

The display unit 304 displays information under  
10 control of the control unit 306.

#### 1.5. Operations of the Content Playback System 1

Operations of the content playback system 1 are described below.

##### (1) Content Playback Start Operation

15 FIG. 12 is a flowchart of an operation of the playback device 100 at the start of content playback.

Upon receiving power from the power supply unit (S103), a playback operation from the remote control 112 via the reception unit 106 (S101-S102), or a signal indicating  
20 detection of insertion of the recording medium 200 from the drive unit 101 (S104-S105), the playback control unit 102 outputs a content decryption instruction to the decryption unit 103 (S106). The decryption unit 103 outputs a media key acquisition instruction to the key  
25 control unit 104 (S107). The key control unit 104 outputs

a media key generation instruction to the media key generation unit 105 (S108).

(2) Media Key Generation Operation by the Media key Generation Unit 105

5           FIG. 13 is a flowchart of a media key generation operation by the media key generation unit 105.

          Upon receiving the media key generation instruction from the key control unit 104 (S108), the media key generation unit 105 reads the device information 141 from  
10   the device information storage unit 111 (S121).

          Next, the media key generation unit 105 attempts to read one set of media information from the media information table 280 on the recording medium 200 (S122). If all sets of media information have already been read from the media  
15   information table 280 (S123: YES), the media key generation unit 105 outputs media key generation failure notification to the key control unit 104 (S141), since the same device information as the device information 141 is not included in the media information table 280. The key control unit  
20   104 outputs media key acquisition failure notification to the decryption unit 103 (S142). The decryption unit 103 outputs decryption failure notification to the playback control unit 102 (S143). The playback control unit 102 terminates the subsequent content playback operation  
25   (S144).

If any set of media information has not yet been read from the media information table 280 (S123:NO), the media key generation unit 105 extracts device information from the read media information (S124), and compares the  
5 extracted device information with the device information 141 (S125). If they do not match (S125:NO), the operation returns to step S122.

If they match (S125:YES), the media key generation unit 105 reads the device key 142 from the device information  
10 storage unit 111 (S126). The media key generation unit 105 also extracts an encrypted media key from the read media information (S127). The media key generation unit 105 decrypts the encrypted media key using the device key 142 (S128), and outputs the decrypted media key to the  
15 key control unit 104 (S129). The key control unit 104 outputs media key acquisition success notification to the decryption unit 103 (S130). The decryption unit 103 outputs the media key acquisition success notification to the playback control unit 102 (S131).

20 (3) Content Playback Control Operation by the Playback Control Unit 102

FIG. 14 is a flowchart of a content playback control operation by the playback control unit 102.

Upon receiving the media key acquisition success  
25 notification from the decryption unit 103 (S131), the

playback control unit 102 reads playback control information having the playback number "1" from the playback path information table 210 (S151). The playback control unit 102 extracts a content name from the read  
5 playback control information (S152), and instructs the decryption unit 103 to decrypt and play back encrypted content identified by the extracted content name (S153). After this, the playback control unit 102 attempts to extract a next playback number from the playback control  
10 information (S154). If the playback control information has no next playback number (S155:NO), the playback control unit 102 ends the operation.

If the playback control information has a next playback number (S155:YES), the playback control unit 102  
15 reads playback control information whose playback number matches the extracted next playback number, from the playback path information table 210 (S156). The playback control unit 102 extracts a content name from the read playback control information (S157), and inquires of the  
20 rights management unit 108 whether encrypted content identified by the extracted content name is playable (S158).

If the rights management unit 108 judges that the content is unplayable (S159:NO), the playback control unit  
25 102 extracts an alternative playback number from the read



playback control information (S163). The playback control unit 102 then reads playback control information whose playback number matches the extracted alternative playback number from the playback path information table 5 210 (S164), and extracts a content name from the read playback control information (S165).

The playback control unit 102 instructs the decryption unit 103 to decrypt and play encrypted content identified by the extracted content name (S160). The 10 playback control unit 102 then attempts to extract a next playback number from the playback control information (S161). If the playback control information has no next playback number (S162:NO), the playback control unit 102 ends the operation.

15 If the playback control information has a next playback number (S162:YES), the playback control unit 102 returns to step S156.

(4) Content Decryption and Playback Operation by the Decryption Unit 103 and the Playback Unit 107

20 FIG. 15 is a flowchart of a content decryption and playback operation by the decryption unit 103 and the playback unit 107.

The decryption unit 103 receives a content name and a decryption and playback instruction from the playback 25 control unit 102 (S170). The decryption unit 103 acquires

a content key from the key control unit 104 (S171), and reads encrypted content identified by the received content name from the recording medium 200 (S172).

Following this, the decryption unit 103 judges  
5 whether the encrypted content contains an encrypted button data table (S173). If the encrypted content does not contain an encrypted button data table (S173:NO), the decryption unit 103 decrypts the encrypted content in units of packets using the acquired content key, and outputs  
10 the decrypted content to the playback unit 107. The playback unit 107 decodes the decrypted content to generate digital video and audio data, and generates analog video and audio signals from the digital video and audio data (S174). The display device 113 outputs the video signal  
15 as video and the audio signal as sounds (S175).

If the encrypted content contains an encrypted button data table (S173:YES), the decryption unit 103 decrypts the encrypted button data table using the acquired content key (S181). The decryption unit 103 then performs steps  
20 S183 to S188 for each set of button data included in the decrypted button data table (S182, S189).

The decryption unit 103 extracts a playback number from the button data (S183). The decryption unit 103 reads a content name corresponding to the extracted playback  
25 number from the playback path information table 210 via

the playback control unit 102 (S184), and inquires of the rights management unit 108 whether content identified by the content name is playable (S185). If the content is judged as being playable (S186:YES), the decryption unit  
5 103 extracts unselected data and selected data that represent normal button display, from the button data (S187). If the content is judged as being unplayable (S186:NO), the decryption unit 103 extracts grayed-out data that represents grayed-out button display, from the  
10 button data (S188).

The decryption unit 103 then decrypts the encrypted content in units of packets using the content key (S190). The decryption unit 103 outputs the decrypted content to the playback unit 107. The decryption unit 103 also outputs  
15 selected data and unselected data or grayed-out data extracted for each set of button data, to the playback unit 107. The playback unit 107 overlays the selected data and unselected data or the grayed-out data on video data to play the content on which the buttons are superimposed.  
20 The display device 113 outputs a video signal as video and an audio signal as sounds (S191).

(5) Content Key Acquisition Operation by the Key Control Unit 104

FIG. 16 is a flowchart of a content key acquisition  
25 operation by the key control unit 104.

The key control unit 104 receives a content key acquisition instruction and a content name from the decryption unit 103 (S200). The key control unit 104 reads key control information having the received content name  
5 from the key control information table 260 on the recording medium 200 (S201), and extracts key generation information from the read key control information (S202).

The key control unit 104 judges whether the key generation information is "00" or not (S203). If the key  
10 generation information is "00" (S203:YES), the key control unit 104 extracts content information from the key control information (S204), and concatenates the decrypted media key received from the media key generation unit 105 and the extracted content information in this order. The key  
15 control unit 104 applies a one-way function to the concatenation outcome to thereby generate a content key (S205), and outputs the content key to the decryption unit 103 (S209).

If the key generation information is not "00"  
20 (S203:NO), the key control unit 104 acquires a rights key corresponding to content identified by the received content name from the rights management unit 108 (S206). The key control unit 104 then judges whether the key generation information is "01" or "10" (S207). If the key generation  
25 information is "10" (S207:NO), the key control unit 104

outputs the rights key to the decryption unit 103 as the content key (S209).

If the key generation information is "01" (S207:YES), the key control unit 104 concatenates the decrypted media  
5 key and the rights key in this order, and applies a one-way function to the concatenation outcome to generate the content key (S208). The key control unit 104 outputs the content key to the decryption unit 103 (S209).

(6) Rights Key Acquisition Operation by the Rights

10 Management Unit 108

FIG. 17 is a flowchart of a rights key acquisition operation by the rights management unit 108.

The rights management unit 108 receives a content key and rights mode information from the key control unit  
15 104 (S221). The rights management unit 108 judges whether the rights mode information is "00" or any of "01", "10", and "01,10", to judge whether any rights mode is specified or not (S222).

If a rights mode is specified, that is, if the rights  
20 mode information is any of "01", "10", and "01,10" (S222:NO), the rights management unit 108 attempts to extract rights information that includes both the rights mode information and the content name from the rights information table  
121 in the rights storage unit 109 (S223).

25 If no rights mode is specified, that is, if the rights

mode information is "00" (S222:YES), the rights management unit 108 attempts to extract rights information that includes the content name from the rights information table 121 (S224).

5           If one or more sets of rights information are extracted as a result (S225:YES), the rights management unit 108 selects one set of rights information (S226). The rights management unit 108 then judges whether the content identified by the content name is playable, based on a  
10   playback count or a playback expiration date included in the selected rights information (S227).

          If the content is judged as being playable (S228:YES), the rights management unit 108 extracts a rights key from the rights information (S229), and outputs the rights key  
15   to the key control unit 104 (S230).

          If the content is judged as being unplayable (S228:NO) or if no set of rights information is extracted (S225:NO), the rights management unit 108 ends the operation.

(7) Playability Judgment Operation by the Key Control Unit  
20   104

          FIG. 18 is a flowchart of a playability judgment operation by the key control unit 104.

          The key control unit 104 receives a content name and a playability judgment instruction from the decryption  
25   unit 103 (S241). The key control unit 104 reads key control

information having the received content name from the key control information table 260 on the recording medium 200 (S242), and extracts key generation information from the read key control information (S243).

5           The key control unit 104 judges whether the key generation information is "00" (S244). If the key generation information is "00" (S244:YES), the key control unit 104 extracts playability information from the key control information (S245), and judges whether the  
10   playability information is "0" or "1" (S246). If the playability information is "1" (S246:"1"), the key control unit 104 notifies the decryption unit 103 that content identified by the content name is playable (S248). If the playability information is "0" (S246:"0"), the key control  
15   unit 104 notifies the decryption unit 103 that the content is unplayable (S247).

          If the key generation information is not "00" (S244:NO), the key control unit 104 extracts the playability information from the key control information  
20   (S249), and judges whether the playability information is "0" or "1" (S250). If the playability information is "1" (S250:"1"), the key control unit 104 notifies the decryption unit 103 that the content is playable (S251). If the playability information is "0" (S250:"0"), the key  
25   control unit 104 extracts rights mode information from

the key control information (S252), and outputs a playability judgment instruction, the rights mode information, and the content name to the rights management unit 108 (S253). The rights management unit 108 judges  
5 whether the content is playable or not (S254). The key control unit 104 receives a judgment result from the rights management unit 108 (S255), and outputs the judgment result to the decryption unit 103 (S256).

#### (8) Playability Judgment Operation by the Rights Management

##### 10 Unit 108

FIG. 19 is a flowchart of a playability judgment operation by the rights management unit 108.

The rights management unit 108 receives a playability judgment instruction, a content name, and rights node  
15 information from the key control unit 104 (S253), and judges whether the rights mode information is "00" or any of "01", "10", and "01,10" (S261). If the rights mode information is any of "01", "10", and "01,10", that is, if a rights mode is specified for content identified by the content  
20 name (S261:NO), the rights management unit 108 attempts to extract rights information that includes both the rights mode information and the content name from the rights information table 121 in the rights storage unit 109 (S262). If the rights mode information is "00", that is, if no  
25 rights mode is specified for the content (S261:YES), the



rights management unit 108 attempts to extract rights information that includes the content name from the rights information table 121 (S263).

If one or more sets of rights information are extracted  
5 as a result (S264:YES), the rights management unit 108 selects one set of rights information (S266). The rights management unit 108 then judges whether the content is playable, based on a playback count or a playback expiration date included in the selected rights information (S267).  
10 If the content is judged as being playable (S268:YES), the rights management unit 108 notifies the key control unit 104 that the content is playable (S269).

If the content is judged as being unplayable (S268:NO), the rights management unit 108 notifies the key control  
15 unit 104 that the content is unplayable (S265).

If no set of rights information is extracted (S264:NO), the rights management unit 108 notifies the key control unit 104 that the content is unplayable (S265).

(9) Operation of Acquiring Rights Information from the  
20 License Server Device 300

FIG. 20 is a flowchart of an operation of acquiring rights information from the license server device 300.

The communication unit 110 in the playback device 100 establishes an encrypted channel, namely a SAC, with  
25 the communication unit 301 in the license server device

300 (S301)..

The communication unit 110 then requests transmission of rights from the communication unit 301 (S302).

The rights generation unit 303 in the license server  
5 device 300 generates rights information for the playback device 100 (S303), and encrypts the generated rights information (S304). The rights generation unit 303 transmits the encrypted rights information to the playback device 100 via the communication control unit 302, the  
10 communication unit 301, and the internet 10 (S305).

The communication unit 110 decrypts the encrypted rights information (S306), and writes the decrypted rights information to the rights storage unit 109 (S307).

#### 1.6. Modifications

15 Although the present invention has been described by way of the above embodiment, it should be obvious that the present invention is not limited to the above. Example modifications are given below.

(1) The above embodiment describes playback path  
20 control according to playback control information and grayed-out button display, as two examples of playback control that is exercised according to license-based content playability, though the present invention is not limited to such. For example, the following modifications  
25 (i) to (iii) are possible.

(i) The recording medium 200 may store standard-version content that can be used by purchasing the recording medium 200, and director's-cut-version content that can be used only by further purchasing special rights. In the playback path information table 210 shown in FIG. 3, the next playback number 219 designates playback control information corresponding to the director's-cut-version content, whilst the alternative playback number 220 designates playback control information corresponding to the standard-version content.

Also, the recording medium 200 may store purchase guidance content which contains an image for purchase of content, and commercial content which contains an advertising message. If the user does not have a license for the content or the playback expiration date of the content is exceeded, the purchase guidance content or the commercial content is played back mandatorily. Also, an operation of acquiring the license from the license server device 300 may be carried out mandatorily.

Furthermore, if the user does not have the license or the playback expiration date is exceeded, any of special playback, menu display, angle switching, and stream switching may be prohibited.

(ii) Playback control according to license-based

content playability may be applied to angle switching in DVDs.

In more detail, the recording medium 200 stores a plurality of pieces of angle content which are subjected to angle switching. These pieces of angle content are grouped according to playback point. All pieces of angle content belonging to one angle content group are playable at one playback point and so one piece of angle content is selected and played back at that playback point. All pieces of angle content belonging to another angle content group are playable at another playback point and so one piece of angle content is selected and played back at that playback point. In the playback path information table 210 shown in FIG. 3, playback control information corresponding to angle content may include a next playback number that designates angle content to be selected next, and an alternative playback number that designates angle content to be selected if the angle content designated by the next playback number is unplayable according to license conditions or the like.

Here, the playback control information may include a plurality of next playback numbers. The playback control information may further include a plurality of alternative playback numbers corresponding to the plurality of next playback numbers.

Information about playability of angle content based on license may be stored, too. In other words, the data structures of the key control information table 260 in FIG. 8 and the rights information table 121 in FIG. 10  
5 can be used in the case of angle switching, too. In this case, each content name in the key control information table 260 and the rights information table 121 identifies angle content.

This makes it possible to prohibit switching to an  
10 unusable angle.

This modification can be summarized as follows. A plurality of pieces of angle content which are subjected to angle switching are recorded on the recording medium 200 in advance. The playback control unit 102 in the  
15 playback device 100 receives an instruction to play angle content, and the rights management unit 108 judges whether the angle content is playable based on corresponding rights information in the rights information table 121.

Depending on a judgment result of the rights management  
20 unit 108, the playback control unit 102 selects angle content to be played next, from an appropriate angle content group on the recording medium 200. The decryption unit 103 and the playback unit 107 decrypt and play the selected angle content.

25 (iii) Likewise, playback control according to

license-based content playability may be applied to audio/subtitle stream switching. This makes it possible to prohibit switching to an unusable audio/subtitle stream. Audio/subtitle streams referred to here are auxiliary (accessory) content that is played back and output together with video content.

The recording medium 200 may store a plurality of pieces of auxiliary content which are grouped according to playback point or playback section. All pieces of auxiliary content belonging to one auxiliary content group are playable at one playback point or playback section. For example, English audio data, Japanese audio data, and Chinese audio data belong to such an auxiliary content group. At the playback point or playback section, one of these pieces of auxiliary content is selected and played back.

Also, all pieces of auxiliary content belonging to another auxiliary content group are playable at another playback point or playback section.

Suppose English audio data, Japanese audio data, and Chinese audio data are recorded on the recording medium 200 in correspondence with each piece of content, and the use of the English audio data and the Chinese audio data is permitted by license whereas the use of the Japanese audio data is not permitted by license. This being the

case, the English audio data may be played back instead of the Japanese audio data.

Also, suppose English subtitle data, Japanese subtitle data, and Chinese subtitle data are recorded on the recording medium 200 in correspondence with each piece of content, and only the use of the English subtitle data is permitted by license. This being the case, the English subtitle data may be played back instead of the Japanese or Chinese subtitle data.

Which is to say, when the recording medium 200 stores a plurality of pieces of auxiliary content, playback control information corresponding to content in the playback path information table 210 includes an auxiliary number for identifying auxiliary content to be played together with the content, and an alternative auxiliary number for identifying auxiliary content to be played if the auxiliary content identified by the auxiliary number is unplayable according to license or the like.

Information about playability of auxiliary content according to license may be stored, too. In other words, the data structures of the key control information table 260 in FIG. 8 and the rights information table 121 in FIG. 10 may be applied to auxiliary content, too. In this case, each content name in the key control information table 260 and the rights information table 121 identifies

auxiliary content.

This modification can be summarized as follows. A plurality of pieces of auxiliary content such as audio streams and subtitle streams are recorded on the recording medium 200. The playback control unit 102 in the playback device 100 receives an instruction to play auxiliary content. The rights management unit 108 judges whether the auxiliary content is playable, based on corresponding rights information in the rights information table 121. Depending on a judgment result of the rights management unit 108, the playback control unit 108 selects auxiliary content to be played next, from an appropriate auxiliary content group on the recording medium 200. The decryption unit 103 and the playback unit 107 decrypt and play back the selected auxiliary content.

(2) The above embodiment describes the case where the key control information table 260 shown in FIG. 8 is stored on the recording medium 200 in unencrypted form, but this is not a limit for the present invention. To prevent unauthorized playback or copying by tampering with playability information or copyability information in the key control information table 260, the key control information table 260 may be encrypted or the like. In this case, it is effective to encrypt the key control information table 260 using the media key. Hence the



playability information and the copyability information in the key control information table 260 can be protected from tampering.

(3) The above embodiment describes an example of playing back content recorded on the recording medium 200, but the same method can be used when copying the content recorded on the recording medium 200.

Which is to say, when the user requests copying of the content recorded on the recording medium 200, a recording device which has the same construction as the playback device 100 acquires a decrypted media key in the same way as in FIG. 13. The recording device then judges the copyability of the content in the same way as in FIG. 14, and copies the content to another recording medium if judged as being copyable.

(4) A content recording/playback system 1b is explained below, as a modification to the above embodiment.

FIG. 21 shows a construction of the content recording/playback system 1b. In the drawing, the content recording/playback system 1b is roughly made up of a recording/playback device 100b and a license server device 300b, which are connected via the internet 10. Also, a recording medium 200b is connected to the recording/playback device 100b by the user.

The recording medium 200b stores a media ID 501 unique

to the recording medium 200b, beforehand.

The license server device 300b stores a key K 521, a content key 531, and content 532 beforehand.

The license server device 300b acquires the media  
5 ID 501 from the recording medium 200b, via the  
recording/playback device 100b and the internet 10 (S401).  
The license server device 300b reads the key K 521 (S402),  
and concatenates the media ID 501 and the key K 521 in  
this order to generate a concatenation key K' 522 (S403).

10 The license server device 300b then reads the content  
key 531, and applies an encryption algorithm to the content  
key 531 using the concatenation key K' 522 to generate  
an encrypted content key 533 (S404). The license server  
device 300b writes the encrypted content key 533 to the  
15 recording medium 200b via the internet 10 and the  
recording/playback device 100b, as an encrypted content  
key 511 (S406). The license server device 300b also reads  
the content 532, and applies an encryption algorithm to  
the content 532 using the content key 531 to generate  
20 encrypted content 534 (S405). The license server device  
300b writes the encrypted content 534 to the recording  
medium 200b via the internet 10 and the recording/playback  
device 100b, as encrypted content 512 (S407).

After this, the recording/playback device 100b reads  
25 the media ID 501 from the recording medium 200b (S421),

and acquires the key K 521 from the license server device 300b via the internet 10 (S422). The recording/playback device 100b concatenates the media ID 501 and the key K 521 in this order to generate a concatenation key K' 541 (S423). The recording/playback device 100b reads the encrypted content key 511 from the recording medium 200b (S424), and applies a decryption algorithm to the encrypted content key 511 using the concatenation key K' 541 to generate a decrypted content key 542 (S426). The recording/playback device 100b also reads the encrypted content 512 from the recording medium 200b (S425), and applies a decryption algorithm to the encrypted content 512 using the decrypted content key 542 to generate decrypted content 543 (S427). The recording/playback device 100b plays back the decrypted content 543 (S428), and displays it (S429).

In this content recording/playback system 1b, the recording/playback device 100b writes the encrypted content key 511 and the encrypted content 512 to the recording medium 200b and reads the encrypted content key 511 and the encrypted content 512 from the recording medium 200b. However, the present invention is not limited to this.

For example, the content recording/playback system 1b may include a recording device and a playback device,

instead of the recording/playback device 100b. In this case, the recording device writes the encrypted content key and the encrypted content output from the license server device 300b to the recording medium 200b, and the playback  
5 device reads the encrypted content key and the encrypted content from the recording medium 200b and plays back the encrypted content.

(5) The above embodiment describes the case where if content is judged as being unplayable, the same playback  
10 control is uniformly exercised regardless of why the content is unplayable. This can be modified as follows.

For instance, different playback control may be performed depending on whether the user does not have a license for content or a playback expiration date of the  
15 content is exceeded. If the user does not have the license, content shown by an alternative playback number is played back, as in the above embodiment. If the playback expiration date is exceeded, on the other hand, the original content is played back while displaying a message  
20 indicating that the playback expiration date is exceeded, or alternatively, purchase guidance content is played back.

Also, playback control information in the playback path information table 210 may include a next playback number, a first alternative playback number, and a second  
25 alternative playback number. As one example, the first

alternative playback number designates playback control information to be used when the user does not have the license, whilst the second alternative playback number designates playback control information to be used when the playback expiration date is exceeded. In this case, the playback control unit 102 uses the next playback number if the playback of the content is permitted by license, the first alternative playback number if the user does not have the license, and the second alternative playback number if the playback expiration date is exceeded.

Which is to say, the playback path information table 210 shown in FIG. 3 includes both the first alternative playback number and the second alternative playback number, so that the playback control unit 102 uses an appropriate alternative playback number depending on why the content is unplayable.

The playback control information may further include a third alternative playback number, a fourth alternative playback number, .... The playback control unit 102 selects an appropriate alternative playback number depending on license conditions.

Also, the rights management unit 108, the rights storage unit 109, and the communication unit 110 in the playback device 100 may be realized by a removable device such as a card. In this case, if the removable device is

not connected to the playback device 100, an inquiry made to the rights management unit 108 will end up being a failure. Different playback control may be exercised in such a case.

(6) The above embodiment describes the case where only the playability of content is judged in the content key acquisition operation and the rights key acquisition operation, but this is not a limit for the present invention.

For example, key control information in the key control information table 260 shown in FIG. 8 and rights information in the rights information table 121 shown in FIG. 10 may include playback quality information about a playback quality of a video or audio stream, in addition to playability information.

Such information may be used in the content key acquisition operation and the rights key acquisition information, as follows. The key control unit 104 writes playback quality information included in rights information over playback quality information included in corresponding key control information, to prioritize the former playback quality information over the latter playback quality information. The key control unit 104 outputs the written playback quality information to the playback unit 107 via the decryption unit 103, and the playback unit 107 plays back the content with a playback quality shown by the received playback quality information.

This makes it possible to have the playback unit 107 down-convert content from HD to SD or QCIF (Quarter Common Intermediate Format) and plays back the content.

(7) The above embodiment describes the case where  
5 rights information in the rights information table 121 shown in FIG. 10 includes rights mode information. According to this construction, however, there is a danger that the rights mode information may be tampered with. Different rights modes are usually managed by different  
10 companies, with there being a possibility that a malicious company may conduct an unauthorized act against another company.

This problem can be avoided by digitally signing rights information which includes rights mode information  
15 and other data, attaching the resulting signature data to the rights information and other data, and including them into a certificate of a signer.

For instance, such a certificate includes a serial number of the certificate, the rights information including  
20 the rights mode information, an identification code of the signer, a signed date, an expiration date of the certificate, and the signature data. The signature data is created by digitally signing the serial number, the rights information, the identification code, the signed  
25 date, and the expiration date using a private key of the

signer.

To use the rights information, the playback device 100 obtains a public key of the signer, and verifies the signature data and other data included in the certificate using the obtained public key to judge whether the rights information has been tampered with. Only if the rights information has not been tampered with, the playback device 100 proceeds to use the rights information.

Also, the key control unit 104 and the rights management unit 108 in the playback device 100 may perform mutual authentication using a SAC. If the mutual authentication has failed, the key control unit 104 and the rights management unit 108 terminate the subsequent information transfer. If the mutual authentication has succeeded, the key control unit 104 and the rights management unit 108 perform the subsequent information transfer. Here, the key control unit 104 and the rights management unit 108 may each be realized by a discrete, removable module independent of the playback device 100.

In such a case, the key control unit 104 may extract the rights mode information from the certificate received during the mutual authentication, and check whether the extracted rights mode information matches rights mode information included in corresponding key control information.



When performing the mutual authentication, a CRL (Certificate Revocation List) showing information for identifying invalid modules may be stored in each of the recording medium 200 and the rights storage unit 109. Such  
5 a CRL allows each of the key control unit 104 and the rights management unit 108 to avoid an invalid module.

As an alternative, the key control unit 104 may hold a first module identifier for identifying an invalid module. In this case, the key control unit 104 acquires an identifier  
10 for identifying the rights management unit 108, and judges whether the acquired identifier matches the first module identifier. If they match, the key control unit 104 refuses to conduct information transfer with the rights management unit 108.

15 Also, the recording medium 200 may store a second module identifier for identifying an invalid module. In this case, the rights management unit 108 reads the second module identifier from the recording medium 200, acquires an identifier for identifying the key control unit 104,  
20 and judges whether the acquired identifier matches the second module identifier. If they match, the rights management unit 108 refuses to conduct information transfer with the key control unit 104.

(8) The above embodiment describes the case where  
25 content is unconditionally judged as being unplayable if

key control information corresponding to the content includes key generation information which shows "media key" and playability information which shows "unplayable". However, the present invention is not limited to this.

5 Even when the key generation information shows "media key" and the playability information shows "unplayable", the key control unit 104 may further inquire of the rights management unit 108 whether the content is playable or not.

10 (9) The above embodiment describes the case where the key control information table 260 is stored on the recording medium 200 separately from encrypted content, but this is not a limit for the present invention.

For example, key control information may be  
15 multiplexed with encrypted content that is identified by a content name included in the key control information. This clarifies the correspondence between the key control information and the encrypted content, thereby making it unnecessary to include the content name in the key control  
20 information. The playback device 100 can acquire the key control information by separating it from the encrypted content.

Also, the key control information table 260 may be stored on a recording medium different from the recording  
25 medium 200. Alternatively, the key control information

table 260 may be acquired via a network. This is particularly effective in the case where not all pieces of content are recorded on one package medium but additional content is separately acquired from a network and recorded  
5 on an HDD.

(10) The above embodiment describes the case where rights information in the rights information table 121 shown in FIG. 10 includes a content name which shows a filename of content, but the present invention is not  
10 limited to this.

As one example, the rights information (also referred to as contract information) includes a rights identifier (also referred to as a license identifier or a contract identifier) for identifying the rights information, with  
15 the rights identifier being also included in corresponding key control information in the key control information table 260 shown in FIG. 8. Based on this rights identifier, the rights management unit 108 searches for the rights information.

20 The rights identifier may also be included in corresponding playback control information in the playback path information table 210 shown in FIG. 3. Through the use of the rights identifier, the playback control unit 102 can inquire of the rights management unit 108, via  
25 the decryption unit 103 and the key control unit 104, whether

the content is playable or not, and use a judgment result of the rights management unit 108.

As can be seen from FIG. 3, the playback control information includes a content name, i.e., a content  
5 identifier for identifying the content. Accordingly, the recording medium 200 may store a correspondence table of content identifiers and rights identifiers. The playback control unit 102 extracts the content identifier from the  
10 playback control information, reads the rights identifier corresponding to the extracted content identifier from the correspondence table, and uses the rights identifier to inquire of the rights management unit 108, via the decryption unit 103 and the key control unit 104, whether the content is playable or not.

15 (11) The above embodiment describes the case where rights information is acquired from the license server device 300, but the present invention is not limited to this. For instance, the rights information table 121 may be stored on the recording medium 200, so that the playback  
20 device 100 reads the rights information table 121 from the recording medium 200. Alternatively, the rights information table 121 may be stored on another recording medium, so that the playback device 100 reads the rights information table 121 from the other recording medium.

25 (12) The above embodiment describes the case where

the functions of the playback control unit 102, the decryption unit 103, the key control unit 104, the media key generation unit 105, and the rights management unit 108 in the playback device 100 can be achieved by the CPU operating in accordance with the computer programs, though this is not a limit for the present invention. For instance, each of the playback control unit 102, the decryption unit 103, the key control unit 104, the media key generation unit 105, and the rights management unit 108 may be realized by separate hardware.

(13) The above embodiment describes a BD as one example of the recording medium 200. The BD has a file system such as a UDF (Universal Disk Format), so that the information recorded on the recording medium 200 shown in FIG. 2 is typically treated as one or more files on the file system. However, this is not a limit for the present invention.

For instance, the media information table 280 may be stored in a specific area of a lead-in area of the BD or in a user data area of the BD. Alternatively, the media information table 280 may be stored in a BCA (Burst Cutting Area). Also, the media key may be generated as follows. An error intentionally created for error detecting code is set as a first media key. Meanwhile, a second media key is encrypted using device information of each playback device and stored in the media information table 280 that

is written in the lead-in area or the user data area. The media key is calculated by applying a one-way function or the like to the first and second media keys.

Also, identification information unique to the recording medium 200, which is stored in the BCA, may be used as the media key of the recording medium 200. As an alternative, identification information unique to a title, which is stored in the lead-in area or the user data area, may be used as the media key of the recording medium 200. Further, a random value stored in the user data area may be used as the media key of the recording medium 200.

Also, an MKB (Media Key Block) stored in the lead-in area or the user data area may be used as information unique to the recording medium 200.

(14) The above embodiment describes the case where rights mode information included in key control information in the key control information table 260 shown in FIG. 8 specifies one or more rights modes specified for corresponding content when key generation information in the key control information is "10" (rights key) or "01" (composite key). Meanwhile, the rights mode information does not specify any rights mode with the value "00", if the key generation information is "00" (media key). This, however, is not a limit for the present invention.

As one example, the rights mode information "00"

indicates a rights mode that depends on a recording medium, whereas the rights mode information "10" or "01" indicates a rights mode that depends on a license. If the rights mode information is "00", the playback device 100 uses  
5 a media key to generate a content key. If the rights mode information is "10" or "01", the playback device 100 uses a rights key or a composite key to generate the content key.

(15) The present invention relates to a terminal for  
10 playing back a medium that stores encrypted content, usability of which is determined according to a license, and playback control information for the encrypted content. The terminal includes a usability inquiry unit, a playback control unit, a license key acquisition unit, and a  
15 decryption unit. The usability inquiry unit inquires whether the encrypted content is permitted to be used according to the license. The playback control unit controls playback based on a result of the inquiry by the usability inquiry unit and the playback control information.  
20 The license key acquisition unit acquires a license key from the license. The decryption unit decrypts the encrypted content using the license key acquired by the license key acquisition unit.

Also, the present invention relates to a terminal  
25 for playing back a medium that stores encrypted content,

usability of which is determined according to a license,  
and playback control information for the encrypted content.  
The playback control information referred to here includes  
at least playback path information for the encrypted  
5 content. The terminal includes a usability inquiry unit,  
a playback control unit, a license key acquisition unit,  
and a decryption unit. The usability inquiry unit inquires  
whether the encrypted content is permitted to be used  
according to the license. The playback control unit  
10 controls a playback path based on a result of the inquiry  
by the usability inquiry unit and the playback control  
information. The license key acquisition unit acquires  
a license key from the license. The decryption unit  
decrypts the encrypted content using the license key  
15 acquired by the license key acquisition unit.

Here, the playback control information may include  
a content identifier for identifying the encrypted content.  
Through the use of this content identifier, the usability  
inquiry unit and/or the license key acquisition unit can  
20 perform the inquiry and/or the license key acquisition.

Here, the playback control information may include  
a license identifier for identifying the license. Through  
the use of this license identifier, the usability inquiry  
unit and/or the license key acquisition unit can perform  
25 the inquiry and/or the license key acquisition.



Also, the present invention relates to a method for playing back a medium that stores encrypted content, usability of which is determined according to a license, and playback control information for the encrypted content.

5 The method includes a usability inquiry step, a playback control step, a license key acquisition step, and a decryption step. The usability inquiry step inquires whether the encrypted content is permitted to be used according to the license. The playback control step  
10 controls playback based on a result of the inquiry by the usability inquiry step and the playback control information. The license key acquisition step acquires a license key from the license. The decryption step decrypts the encrypted content using the license key acquired by the  
15 license key acquisition step.

Also, the present invention relates to a method for playing back a medium that stores encrypted content, usability of which is determined according to a license, and playback control information for the encrypted content.  
20 The playback control information referred to here includes at least playback path information for the encrypted content. The method includes a usability inquiry step, a playback control step, a license key acquisition step, and a decryption step. The usability inquiry step inquires  
25 whether the encrypted content is permitted to be used

according to the license. The playback control step controls a playback path based on a result of the inquiry by the usability inquiry step and the playback control information. The license key acquisition step acquires  
5 a license key from the license. The decryption step decrypts the encrypted content using the license key acquired by the license key acquisition step.

(16) The present invention relates to a terminal for playing back a medium on which encrypted content and a  
10 media key unique to the medium are stored. The terminal includes a license acquisition unit, a license key acquisition unit, a key generation unit, and a decryption unit. The license acquisition unit acquires a license including at least a key for decrypting the encrypted  
15 content. The license key acquisition unit acquires a license key from the license. The key generation unit generates a content key from the media key and the license key. The decryption unit decrypts the encrypted content using the content key.

20 Also, the present invention relates to a terminal for playing back a medium on which encrypted content and a media key unique to the medium are stored. The terminal includes a license acquisition unit, a license key acquisition unit, a key generation unit, a usability  
25 judgment unit, and a decryption unit. The license

acquisition unit acquires a license including at least a key for decrypting the encrypted content and a use condition of the encrypted content. The license key acquisition unit acquires a license key from the license.

5 The key generation unit generates a content key from the media key and the license key. The usability judgment unit judges whether the encrypted content corresponding to the license is permitted to be used, based on the use condition. The decryption unit decrypts the encrypted content using

10 the content key, if the encrypted content is judged as being permitted to be used.

Also, the present invention relates to a terminal for playing back a medium on which encrypted content, a media key unique to the medium, and processing control

15 information are stored. The terminal includes a license acquisition unit, a license key acquisition unit, a key generation unit, a key judgment unit, and a decryption unit. The license acquisition unit acquires a license including at least a key for decrypting the encrypted

20 content. The license key acquisition unit acquires a license key from the license. The key generation unit generates a content key from the media key and the license key. The key judgment unit judges whether the license key or the content key is to be used for decrypting the encrypted

25 content, based on the processing control information. The

decryption unit decrypts the encrypted content using the key determined by the key judgment unit.

Here, the processing control information may include a content identifier for identifying the encrypted content, and key type information showing whether the license key or the content key is to be used.

Here, the processing control information may be multiplexed with the encrypted content.

Also, the present invention relates to a method for playing back a medium on which encrypted content and a media key unique to the medium are stored. The method includes a license acquisition step, a license key acquisition step, a key generation step, and a decryption step. The license acquisition step acquires a license including at least a key for decrypting the encrypted content. The license key acquisition step acquires a license key from the license. The key generation step generates a content key from the media key and the license key. The decryption step decrypts the encrypted content using the content key.

Also, the present invention relates to a method for playing back a medium on which encrypted content and a media key unique to the medium are stored. The method includes a license acquisition step, a license key acquisition step, a key generation step, a usability

judgment step, and a decryption step. The license acquisition step acquires a license including at least a key for decrypting the encrypted content and a use condition of the encrypted content. The license key acquisition step acquires a license key from the license. 5 The key generation step generates a content key from the media key and the license key. The usability judgment step judges whether the encrypted content corresponding to the license is permitted to be used, based on the use condition. 10 The decryption step decrypts the encrypted content using the content key, if the encrypted content is judged as being permitted to be used.

Also, the present invention relates to a method for playing back a medium on which encrypted content, a media key unique to the medium, and processing control 15 information are stored. The method includes a license acquisition step, a license key acquisition step, a key generation step, a key judgment step, and a decryption step. The license acquisition step acquires a license including at least a key for decrypting the encrypted content. The license key acquisition step acquires a license key from the license. The key generation step generates a content key from the media key and the license key. The key judgment step judges whether the media key 20 or the content key is to be used for decrypting the encrypted 25

content, based on the processing control information. The decryption step decrypts the encrypted content using the key determined by the key judgment step.

(17) The present invention relates to a terminal for playing back a medium on which encrypted content and a media key unique to the medium are stored. The terminal includes a license acquisition unit, a content key acquisition unit, a key selection unit, and a decryption unit. The license acquisition unit acquires a license including at least a key for decrypting the encrypted content. The content key acquisition unit acquires a content key from the license. The key selection unit selects one of the media key and the content key for decrypting the encrypted content. The decryption unit decrypts the encrypted content using the key selected by the key selection unit.

Also, the present invention relates to a terminal for playing back a medium on which encrypted content, a media key unique to the medium, and key selection information are stored. The terminal includes a license acquisition unit, a content key acquisition unit, a key selection unit, and a decryption unit. The license acquisition unit acquires a license including at least a key for decrypting the encrypted content. The content key acquisition unit acquires a content key from the license.

The key selection unit selects one of the media key and the content key for decrypting the encrypted content, based on the key selection information. The decryption unit decrypts the encrypted content using the key selected by  
5 the key selection unit.

Also, the present invention relates to a terminal for playing back a medium on which encrypted content, a media key unique to the medium, and key selection information are stored. The terminal includes a license  
10 acquisition unit, a content key acquisition unit, a key selection unit, a usability judgment unit, and a decryption unit. The license acquisition unit acquires a license including at least a key for decrypting the encrypted content and a use condition of the encrypted content. The  
15 content key acquisition unit acquires a content key from the license. The key selection unit selects one of the media key and the content key for decrypting the encrypted content, based on the key selection information. The usability judgment unit judges whether the encrypted  
20 content corresponding to the license is permitted to be used, based on the use condition. The decryption unit decrypts the encrypted content using the key selected by the key selection unit, if the encrypted content is judged as being permitted to be used.

25 Here, the key selection information may include a

content identifier for identifying the encrypted content, and key type information showing whether the media key or the content key is to be used.

Here, the key selection information may be  
5 multiplexed with the encrypted content.

Here, the key selection information may include a license identifier for identifying the license corresponding to the encrypted content, so that the content key acquisition unit can acquire the content key from the  
10 license identified by the license identifier.

Also, the present invention relates to a method for playing back a medium on which encrypted content and a media key unique to the medium are stored. The method includes a license acquisition step, a content key  
15 acquisition step, a key selection step, and a decryption step. The license acquisition step acquires a license including at least a key for decrypting the encrypted content. The content key acquisition step acquires a content key from the license. The key selection step  
20 selects one of the media key and the content key for decrypting the encrypted content. The decryption step decrypts the encrypted content using the key selected by the key selection step.

Also, the present invention relates to a method for  
25 playing back a medium on which encrypted content, a media



key unique to the medium, and key selection information are stored. The method includes a license acquisition step, a content key acquisition step, a key selection step, and a decryption step. The license acquisition step acquires  
5 a license including at least a key for decrypting the encrypted content. The content key acquisition step acquires a content key from the license. The key selection step selects one of the media key and the content key for decrypting the encrypted content, based on the key  
10 selection information. The decryption step decrypts the encrypted content using the key selected by the key selection step.

Also, the present invention relates to a method for playing back a medium on which encrypted content, a media  
15 key unique to the medium, and key selection information are stored. The method includes a license acquisition step, a content key acquisition step, a key selection step, a usability judgment step, and a decryption step. The license acquisition step acquires a license including at  
20 least a key for decrypting the encrypted content and a use condition of the encrypted content. The content key acquisition step acquires a content key from the license. The key selection step selects one of the media key and the content key for decrypting the encrypted content, based  
25 on the key selection information. The usability judgment

step judges whether the encrypted content corresponding to the license is permitted to be used, based on the use condition. The decryption step decrypts the encrypted content using the key selected by the key selection step, 5 if the encrypted content is judged as being permitted to be used.

Also, the present invention relates to a medium storing encrypted content. The medium also stores a media key unique to the medium, and key selection information 10 showing whether the encrypted content has been generated by performing encryption using the media key or not.

Here, the key selection information may includes a content identifier for identifying the encrypted content.

Here, the key selection information may include a 15 license identifier for identifying a license for the encrypted content.

(18) The above embodiment describes the case where one key control information table is stored on the recording medium 200. However, a plurality of key control 20 information tables may be stored on the recording medium 200.

If the recording medium 200 is a recordable or rewritable medium, the user can add encrypted content to the recording medium 200 which he or she acquired. When 25 adding the encrypted content, a key control information

table corresponding to the added content may need to be stored as well.

In this case, the key control unit 104 searches the plurality of key control information tables on the recording medium 200, for a key control information table  
5 that designates encrypted content which is to be judged as being playable or not. Here, more than one key control information table may designate the encrypted content. In such a case, the key control unit 104 detects the key  
10 control information table to be referenced, according to such a rule that prioritizes a last-stored key control information table.

Further, composite content may be distributed among a plurality of recording media. Especially when the  
15 recording medium 200 is a non-recordable medium, encrypted content that is added later needs to be recorded to another recording medium. A typical example of the other recording medium is an HDD equipped in the playback device 100. The  
20 playback device 100 records the additional encrypted content to the HDD. In this case too, the key control unit 104 searches a plurality of key control information tables on the plurality of recording media that store different parts of the composite content which are related to each other by links, for a key control information table that  
25 is to be referenced.

(19) The construction elements of each of the above devices may be partially or entirely implemented by a single system LSI. The system LSI is an ultra-multifunctional LSI manufactured by integrating multiple components on a single chip, and is actually realized by a computer system that includes a microprocessor, a ROM, and a RAM. A computer program is stored on the RAM. Functions of the system LSI can be achieved by the microprocessor operating in accordance with this computer program.

(20) The construction elements of each of the above devices may be partially or entirely implemented by a removable IC card or a discrete module. The IC card or module referred to here is a computer system that includes a microprocessor, a ROM, and a RAM. The IC card or module may contain the aforementioned ultra-multifunctional LSI. Functions of the IC card or module can be achieved by the microprocessor operating in accordance with the computer program. Here, the IC card or module may be tamper-resistant.

(21) Each of the above devices is actually a computer system that includes a microprocessor, a ROM, and a RAM. A computer program is stored on the RAM. The functions of each device can be achieved by the microprocessor operating in accordance with this computer program. This computer program is constituted by a plurality of sets

of instruction code for a computer to realize the predetermined functions.

(22) The present invention also applies to the method described above. This method may be realized by a computer program that is executed by a computer. Such a computer  
5 program may be distributed as a digital signal.

The present invention may be realized by a computer-readable storage medium, such as a flexible disk, a hard disk, a CD-ROM, an MO, a DVD, a DVD-ROM, a DVD-RAM,  
10 a BD, or a semiconductor memory, on which the above computer program or digital signal is recorded. Conversely, the present invention may also be realized by the computer program or digital signal that is recorded on such a storage medium.

15 The computer program or digital signal that achieves the present invention may also be transmitted via a network, such as an electronic communications network, a wired or wireless communications network, or an internet, or via data broadcasting.

20 The present invention can also be realized by a computer system that includes a microprocessor and a memory. In this case, the computer program can be stored in the memory, with the microprocessor operating in accordance with this computer program.

25 The computer program or digital signal may be provided

to an independent computer system by distributing a storage medium on which the computer program or digital signal is recorded, or by transmitting the computer program or digital signal via a network. The independent computer system may then execute the computer program or digital signal to function as the present invention.

(23) The above embodiment and modifications may be freely combined.

(24) A playback device and playback method for encrypted content and a recording medium on which data used by the above playback device and playback method is stored, to which the present invention relates, are suitable for use in content playback of media which contain both conventional copy-protected content and DRM content, and are therefore useful in such fields as package media and content distribution.

#### INDUSTRIAL APPLICABILITY

The devices and recording medium to which the present invention relates can be used recurrently and continuously in a content delivery industry that produces and delivers content. Also, the devices to which the present invention relates can be manufactured and sold recurrently and continuously in an electrical product manufacturing industry.